Remarks

This responds to the Office action mailed March 25, 2005 ["the Action"]. Reconsideration of the application is respectfully requested in view of the following remarks. Claims 1-18 are pending in the application. No claims have been allowed. No claims are amended. Claims 1, 2, and 13 are independent.

Rejections Under 35 U.S.C. § 102(e)

The Action rejects claims 1-18 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,772,3321 to Hind et al. ["Hind"]. Applicants respectfully submit the claims in their present form are allowable over the cited art. For a 102(e) rejection to be proper, the cited art must show each and every element as set forth in a claim. (*See* MPEP § 2131.) However, the cited art does not describe each and every element. Accordingly, applicants request that all rejections be withdrawn.

Claim 2

Claim 2 recites, in part,

> *securely networking a security-uninitialized device with a branding device via a secured network medium;*
> *transmitting a branding certificate from the branding device to the security-uninitialized device via the secured network medium, ...*
> *transmitting a trust group membership certificate from the branding device to the security-uninitialized device via the secured network medium, the trust group membership certificate authenticating that the security-uninitialized device is a member of the trust group ....*

For example, the Application at Figure 4 and page 8, line 8 to page 9, line 20 describes a branding process.

Claim 2 stands rejected over Hind. However, Hind does not describe, nor does it teach or suggest, each and every element of the claim as required by § 102.

Hind does not teach or suggest a "trust group membership certificate authenticating that the security-uninitialized device is a member of the trust group" because Hind teaches creating individual certificates for each device. In its rejection of the language "trust group membership

certificate" the Action cites to column 10, lines 18-24 of Hind. However, the cited section does not describe any characteristics of the certificate itself and, in fact, describes associating devices with particular groups, *after* the certificates have been created:

> Once a public key, private key and certificate have been created, the administrator can use standard distribution techniques ... to associate the device with a particular user or group of users, the user or user group or device with access control groups and to log device characteristics of the device.

Hind does describe certificate characteristics at column 9, lines 32-51. However, it makes clear that the certificates are created for each individual mobile device and gives no indication that trust group certificates are created:

> The administration server 1001 then *acquires or generates a public/private key pair 1035 for mobile device 1003.* At 1045 the administration server 1001 *puts the created public key 1040 into a certificate request message buffer 1050 along with device 1003's unique identifier 1015*... and sends 1060 the certificate request 1050 that was prepared for mobile device 1003 to the Certificate authority... When the administration server 1001 receives the signed certificate 1050', it ... sends the signed certificate 1050' and the corresponding private key ... to the mobile device 1003 over the secure connection 1080 and sends the Certificate Authority's certificate (containing the CA's public key) to mobile device 1003 as well, and the session is ended.

Thus, Hind describes transmission of a key that is specific to the mobile device, which means Hind does not teach or suggest a trust group membership certificate which authenticates membership in a trust group. Furthermore, Hind's description of the Certificate Authority's certificate is also not a trust group membership certificate, as it is the same for *any* mobile device. Because the Hind's Certificate Authority certificate is not concerned with groups, it cannot authenticate membership in a trust group. Hind therefore does not teach or suggest "trust group membership certificate" which "authenticat[es] that the security-uninitialized device is a member of the trust group" as recited in claim 2.

Hind also cannot teach or suggest "transmitting a branding certificate... via the secured network medium" and "transmitting a trust group membership certificate... via the secured network medium" as recited in claim 2. This is because the section of Hind cited in rejecting the "secured network medium" of claim 2 requires transmission of a device certificate and public and private keys to have previously happened, thus it cannot describe the same "secured network

medium" which claim 2 also recites when transmitting certificates. In its rejection of the language "secured network medium," the Action cites to column 11, lines 5-10:

> FIG. 2 depicts example flows for establishing secure communications between multiple devices each equipped with a radio transceiver using the present invention. *In the preferred embodiment, the FIG. 2 flows occur sometime after each device has been provided with its own Device Certificate, its own private key, and the Certificate Authority's well-known public key, as previously described with respect to FIG. 1. However, the present invention does not exclude providing the data items in some other way.*

However, claim 2 also recites "transmitting a branding certificate from the branding device to the security-uninitialized device *via the secured network medium*," and "transmitting a trust group membership certificate from the branding device to the security-uninitialized device *via the secured network medium*." Thus, the section of Hind cited in the Action cannot describe a "secured network medium" which is used to transmit these certificates when it requires that the certificates be already transmitted if it is to operate. Because of this, Hind appears to actually teach away from the use of a secured network medium to transmit certificates.

For at least these reasons Hind does not teach or suggest every element of claim 2. Therefore claim 2, and its dependent claims 3-12 are allowable at this time. Applicants request that the rejection of claims 2-12 be withdrawn.

Claim 1

Claim 1 recites, in part:

> *electronically imprinting the security-uninitialized device with group membership and cryptographic key data by the branding device via the secured network medium, ...*

In its rejection of claim 1, the Action cites only to the sections cited to in its rejection of claim 2. Furthermore, the Action does not address specific language of claim 1, including the above-quoted language which is not found in claim 2. Thus, the Action does not demonstrate how Hind teaches or suggests the quoted language of claim 1. For at least this reason, as well as the reasons cited above with respect to claim 2, Hind does not teach or suggest every element of claim 1. Claim 1 is allowable at this time. Applicants request that the rejection of claim 1 be withdrawn.

Claim 13

Claim 13 recites, in part:

> a security initializer operational to receive the branding public key from a branding device securely networked to the networked computing device, and further operational to initialize the security resolver with the branding public key.

In its rejection of claim 13, the Action cites only to the sections cited to in its rejection of claim 2. Furthermore, the Action does not address specific language of claim 13, including the above-quoted language which is not found in claim 2. Thus, the Action does not demonstrate how Hind teaches or suggests the quoted language of claim 13. For at least this reason, as well as the reasons cited above with respect to claim 2, Hind does not teach or suggest every element of claim 13. Thus, claim 13, and its dependent claims 14-18, are allowable at this time. Applicants request that the rejection of claims 13-18 be withdrawn.

Conclusion

Claims 1-18 should be allowable. Such action is respectfully requested.

Request for Interview

In view of the preceding amendments and remarks, Applicants believe the application to be allowable. If any issues remain, however, the Examiner is formally requested to contact the undersigned attorney at (503) 226-7391 prior to issuance of the next communication in order to arrange a telephonic interview. This request is being submitted under MPEP § 713.01, which indicates that an interview may be arranged in advance by a written request.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By _____
Stephen A. Wight
Registration No. 37,759

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446